Cellebrite Physical Extraction Manual for iPhone & iPad

July 3rd, 2011

Revision 1.3

Table of Contents

Introduction

This manual provides an overview of the steps required to extract data from an iPhone or iPad using the UFED Physical Analyzer.

The UFED Physical Analyzer allows you to extract, decode and analyze the following devices running iOS version 3.0 or higher:

- **iPhone (original)**
- **iPhone 3G**
- **iPhone 3GS**
- **iPhone 4 GSM**
- **iPhone 4 CDMA**
- **iPad 1**

Before You Start

You will need:

- A UFED Physical Analyzer installed on a PC with Windows XP/Vista/7 Operating Systems (iPhone/iPad physical extraction is not designed to be used in Virtual Machine environments).
- An iPhone or iPad.
- UFED Cable Number 110.

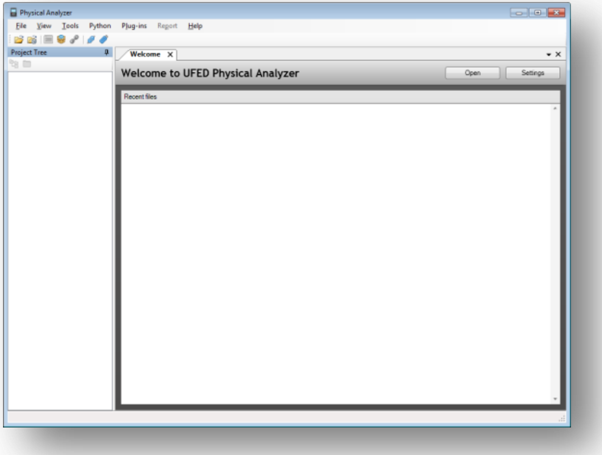
An Internet connection is required before the first use for the installation of updates. Access to the Internet is used to download relevant software and may be carried out through any computer with Internet connection.

Performing an Extraction

The following steps will guide you through the extraction process.

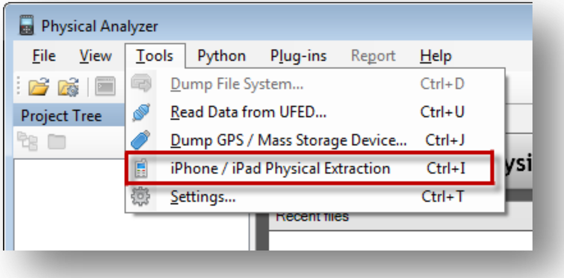
Step 1: Launch the UFED Physical Analyzer

1. Launch UFED Physical Analyzer by clicking the application icon or program shortcut. The default location of UFED Physical Analyzer is: C:\Program Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer.



Step 2: Open iPhone / iPad Physical Extraction

1. Click the *Tools* menu and click *iPhone/iPad Physical Extraction.* “UFED iPhone Physical” will then launch.


Physical Analyzer
File
View
Tools
Python
Plug-ins
Report
Help
Project Tree
Dump File System... Ctrl+D
Read Data from UFED... Ctrl+U
Dump GPS / Mass Storage Device... Ctrl+J
iPhone / iPad Physical Extraction Ctrl+I
Settings... Ctrl+T
Recent files

On first use

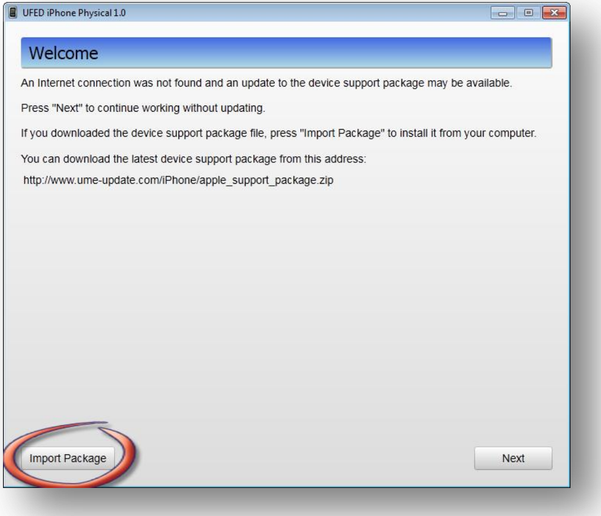
On the first use of UFED iPhone Physical you will be required to download the Apple Device Support Package. The support package contains the newest utilities that enable UFED iPhone Physical to be compatible with a variety of devices. The download may take a while, depending on your Internet connection speed.

No Internet connection?

If your computer is not connected to the Internet you can download the support package on a different computer and manually copy it to your computer.

1. Click this link[1] to download the latest Apple Device Support Package:

2. Copy the file to your computer.
3. Click the *Import Package* button and locate the file on your computer.



Welcome

An Internet connection was not found and an update to the device support package may be available.

Press "Next" to continue working without updating.

If you downloaded the device support package file, press "Import Package" to install it from your computer.

You can download the latest device support package from this address:

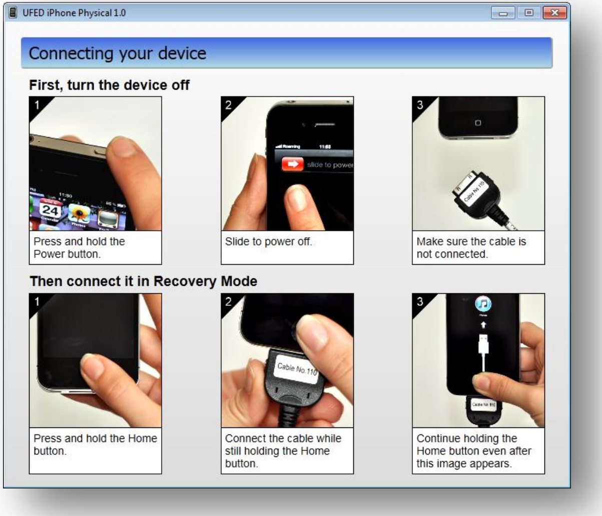
http://www.ume-update.com/iPhone/apple_support_package.zip

[1] http://www.ume-update.com/iPhone/apple_support_package.zip

Step 3: Connect the device in Recovery Mode to your PC

1. Follow the steps on the screen to connect the device in Recovery Mode.

   Note: connect your device to the PC using cable # 110 or the iPhone/iPad data cable.



UFED iPhone Physical 1.0

Connecting your device

First, turn the device off

1 Press and hold the Power button.

2 Slide to power off.

3 Make sure the cable is not connected.

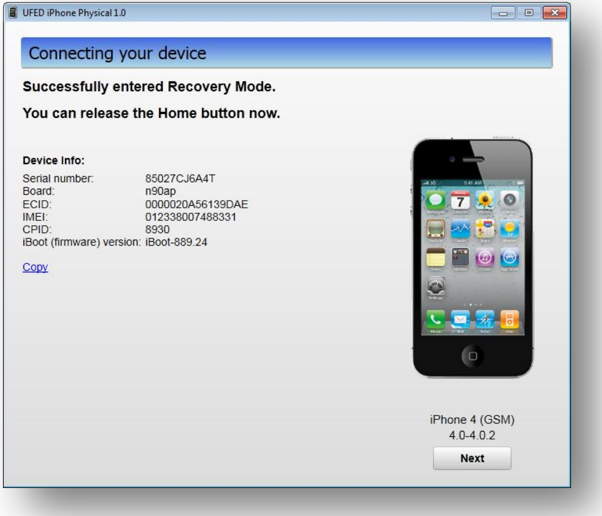
Then connect it in Recovery Mode

1 Press and hold the Home button.

2 Connect the cable while still holding the Home button.

3 Continue holding the Home button even after this image appears.

2. After connecting the device in Recovery Mode, UFED iPhone Physical will display certain device information, such as serial number, IMEI, hardware version, iOS version and more. You can copy that information to the clipboard by clicking the *Copy* link.



Connecting your device

Successfully entered Recovery Mode.

You can release the Home button now.

Device Info:

Serial number:	85027CJ6A4T
Board:	n90ap
ECID:	0000020A56139DAE
IMEI:	012338007488331
CPID:	8930
iBoot (firmware) version:	iBoot-889.24

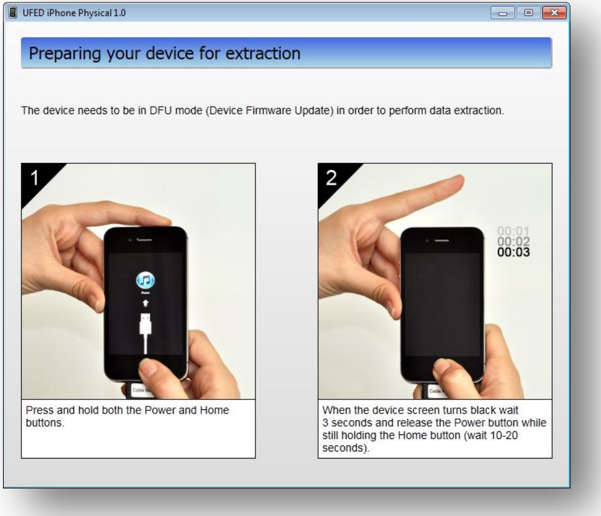
Copy

iPhone 4 (GSM)
4.0-4.0.2

Note: In case a range of versions are displayed, the version of the specific device connected may be any version within the displayed range. In the example above the iOS version may be 4.0, 4.0.1 or 4.0.2.

Step 4: Setting the Device to DFU Mode

1. Click *Next* on the screen with the device info.
2. Follow the instructions on the screen to set the device to DFU (Device Firmware Upgrade) mode. Be assured that UFED iPhone Physical will not affect the device firmware or user data.



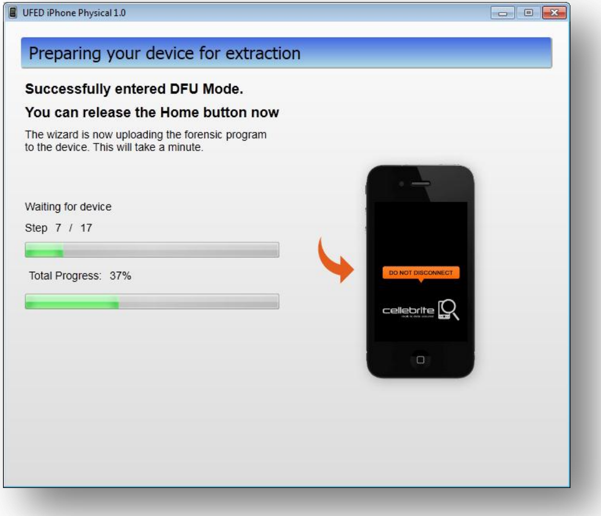
Preparing your device for extraction

The device needs to be in DFU mode (Device Firmware Update) in order to perform data extraction.

Press and hold both the Power and Home buttons.

When the device screen turns black wait 3 seconds and release the Power button while still holding the Home button (wait 10-20 seconds).

3. When you have succeeded, the following screen will be displayed.



UFED iPhone Physical 1.0

Preparing your device for extraction

Successfully entered DFU Mode.

You can release the Home button now

The wizard is now uploading the forensic program to the device. This will take a minute.

Waiting for device

Step 7 / 17

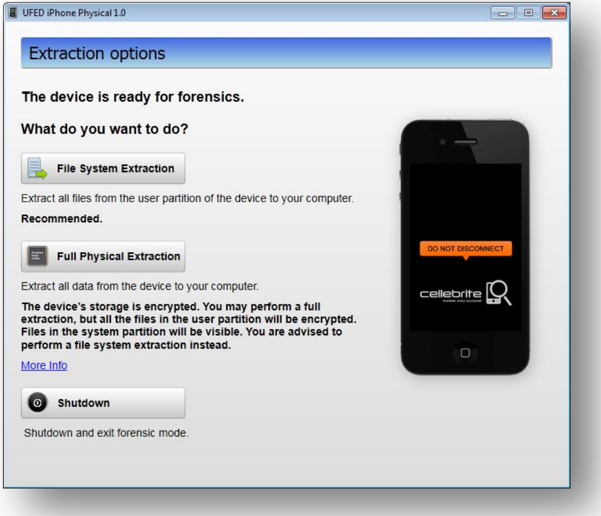
Total Progress: 37%

UFED iPhone Physical will upload the forensics program required to extract data from the device. As mentioned above, this will not affect the data, memory or firmware of the device.

Step 5: Extract Data

Now the device is ready for forensic extraction.

1. Choose the desired extraction method (Full Physical or File System). We recommend reading the Extraction and Encryption FAQ appendix to make the best of your iPhone and iPad extraction.
2. Choose the location you wish to save the extraction to. You can save it on your computer or on a removable storage device.



Extraction options

The device is ready for forensics.

What do you want to do?

File System Extraction

Extract all files from the user partition of the device to your computer.

Recommended.

Full Physical Extraction

Extract all data from the device to your computer.

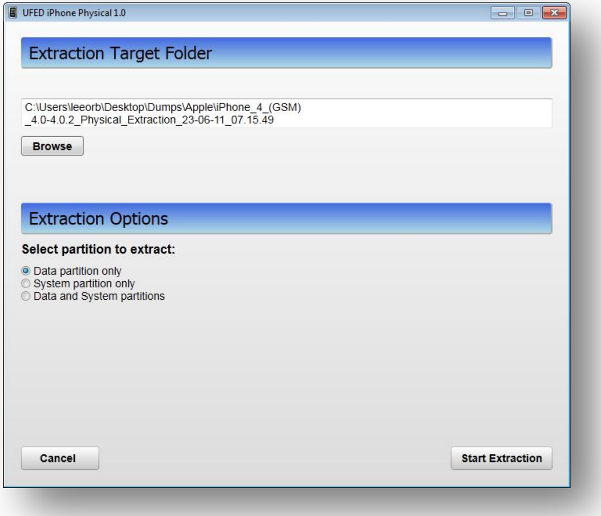
The device's storage is encrypted. You may perform a full extraction, but all the files in the user partition will be encrypted. Files in the system partition will be visible. You are advised to perform a file system extraction instead.

More Info

Shutdown

Shutdown and exit forensic mode.

3. While performing Full Physical Extraction, you will be required to choose the relevant partition for extraction. Select the Data partition, System partition or both partitions.
4. Click Start Extraction.



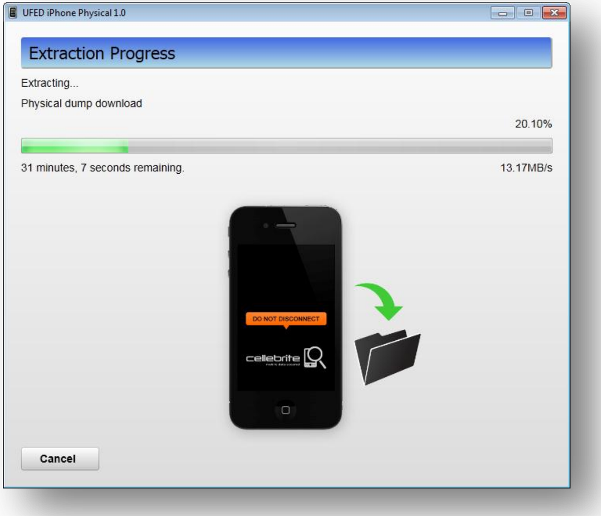
C:\Users\leeorb\Desktop\Dumps\Apple\iPhone_4_(GSM)
_4.0-4.0.2_Physical_Extraction_23-06-11_07.15.49

Select partition to extract:

● Data partition only
○ System partition only
○ Data and System partitions

Step 6: Wait

1. Wait until the extraction is completed. The extraction duration varies depending on the extraction method, the device used, the quantity of data on the device, your computer and other parameters.



UFED iPhone Physical 1.0

Extraction Progress

Extracting...

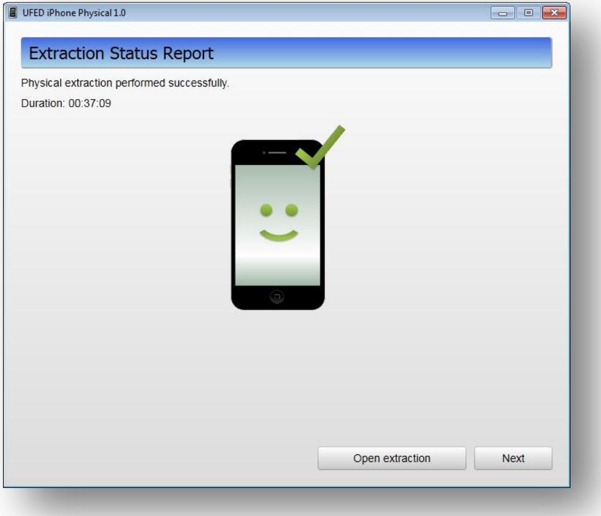
Physical dump download

20.10%

31 minutes, 7 seconds remaining.

13.17MB/s

2. When the extraction is completed you will see this screen.
3. Clicking *Open extraction* will load the extraction file in UFED Physical Analyzer.
4. Clicking *Next* will take you back to the extraction options screen.



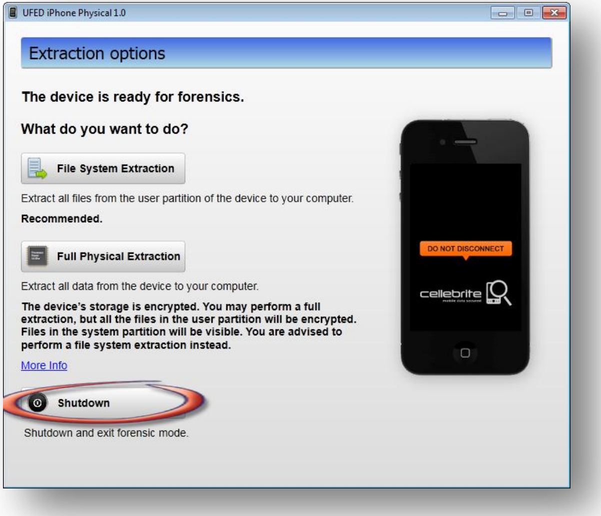
Extraction Status Report

Physical extraction performed successfully.

Duration: 00:37:09

Step 7: Shutdown the Device

1. When extraction is complete, you may click *Shutdown* to safely turn off the device and set it back to normal mode.



The device is ready for forensics.

What do you want to do?

Extract all files from the user partition of the device to your computer.

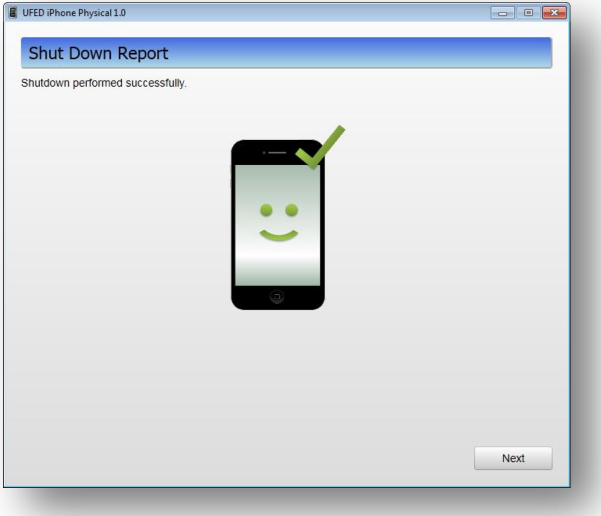
Recommended.

Extract all data from the device to your computer.

The device's storage is encrypted. You may perform a full extraction, but all the files in the user partition will be encrypted. Files in the system partition will be visible. You are advised to perform a file system extraction instead.

Shutdown and exit forensic mode.

2. The *Shut Down Report* screen will indicate your device has successfully been shut down.



Shut Down Report

Shutdown performed successfully.

Appendix - UFED iPhone Physical Extraction and Encryption FAQ

Is it possible to extract data from user locked iPhone devices?

Yes. The UFED iPhone Physical Extraction solution enables extraction of the device image and file system even when user lock is active.

What is "physical extraction"?

Physical extraction is performed by imaging the device’s partitions. This recovers the device's entire file system which can then be decoded by UFED Physical Analyzer. On devices that have data encryption, the contents of the files may be encrypted (explanation below).

What is "low-level file system extraction"?

Apple iOS devices have two partitions: The system partition (normally 1GB) and the user data partition (the rest of the flash memory). The system partition contains the operating system files. The user data partition contains all user-generated content (photos, messages, etc.)

Low-level file system extraction reads the entire directory tree of the user partition and puts it in a simple “tar” file. The user data will not be encrypted in a low-level file system extraction, even if encryption is enabled on the device. However, some "protected" files cannot be fully extracted.

On devices that have data encryption, some files may be protected and inaccessible. Protected files are only readable when the device is turned on regularly and unlocked. Low-level file system extraction cannot extract the contents of those files; only their metadata. Among the protected files are some of the email files.

The system partition is never encrypted, even if encryption is enabled on the device.

What devices have data encryption enabled?

Device	Data Encryption
iPhone (Original), iPhone 3G, iPod Touch 1st and 2nd generation*	Disabled
iPhone 3GS iPod Touch 3rd generation* iPad 1	In some cases. See paragraph below.
iPhone 4 iPod Touch 4th generation* iPad 2*	Enabled

* Extraction from this device is not currently supported.

iPhone 3GS, iPod Touch 3rd Generation and iPad 1 were originally manufactured and shipped with iOS version 3.x. The data encryption feature was added in iOS 4.x.

Simply updating an iOS 3.x device to iOS 4.x (or later) does not enable data encryption. Data encryption will be enabled on these devices only if the user has "restored" the device with iOS 4.x. (or later) "Restore" is a feature in iTunes which reformats the file system (making it encryption-ready) and reinstalls iOS.

If the device had iOS 4.x (or later) preinstalled on it when it was bought, encryption will be enabled.

What type of extracted data will be encrypted?

If data encryption is disabled, all data on the device will be unencrypted and readable. However, if data encryption is enabled, the data that's encrypted varies between the different types of extractions:

Extraction type	If data encryption enabled
Physical extraction - system partition	Will be extracted and not encrypted
Physical extraction - user partition	File contents will be encrypted. Directory tree, file names, modification dates, etc. will not be encrypted
Low-level file system extraction **Non-protected files**	Will be extracted and not encrypted
Low-level file system extraction **Protected files**	File contents will not be extracted. Only 0's will appear. File names, modification dates, etc. will be extracted and not encrypted

What is the best way to extract data from an encrypted device?

The best way to extract data from a device with encryption enabled is to perform a low-level file system extraction. You will be able to retrieve all user content except protected files (among which are some of the email files).

Can jailbreaking help extract data from an encrypted device?

Unfortunately, jailbreaking does not help circumvent the data encryption. The Cellebrite UFED solution performs extraction without Jailbreaking the device. Both Jailbroken and non-jailbroken devices are supported.

Does data extraction affect the storage or data on the device?

No.

The extraction application does not load iOS, but instead loads a special forensic utility to the device. This utility is loaded to the device's memory (RAM) and runs directly from there. Therefore, it does not modify the device's storage and does not leave any footprints.